October 14, 2003

(18)

Public Information Room
Office of the Comptroller of the Currency
250 E Street, SW
Mail Stop 1-5
Washington, DC 20219
Attention: Docket No. 03-18

Ms. Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551
Attn: Docket No. OP-1155

Robert E. Feldman
Executive Secretary
Attention: Comments/OES
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC 20552
Attention: No. 03-35

RE: **Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice**

Ladies and Gentlemen,

FleetBoston Financial Corporation, a diversified financial holding company headquartered in Boston, Massachusetts, ("FleetBoston") is pleased to have this opportunity to comment on the above- reference Proposed Guidance offered for comment.

About Us

FleetBoston is the seventh largest bank holding company in the United States, with total assets exceeding $190 billion. FleetBoston offers a comprehensive array of financial products and services to 20 million customers in more than 20 countries and territories. Among the company's key lines of business are: retail and commercial banking; capital markets, investment banking and commercial finance; trust and investment services, including nationwide brokerage; and private equity investing.

FleetBoston's primary banking subsidiary, Fleet National Bank. (the "Bank"), is a national banking association with branches throughout the Northeast and Middle Atlantic states. The Bank's businesses are national in scope and include consumer, small business and commercial banking, international banking, corporate banking, principal investing, credit card services, commercial real estate lending, commercial leasing and mortgage banking. Some of these businesses are conducted by the Bank through wholly-owned operating subsidiaries.

Overview of Comments

FleetBoston supports the Proposed Guidance's conclusion that an aggressive response program is a key part of an institution's information security plan and also supports the Agencies' efforts to explore measures aimed at enhancing the security of customer information and reducing the harmful effects of identity theft. However, key aspects of the Proposed Guidance do not effectively recognize the day-to-day realities of customer information security and suggest an overly rigid approach. A more balanced and flexible approach is needed to allow financial institutions to develop and implement effective and efficient fraud prevention measures consistent with their overall security procedures and business practices.

During the course of this past year, the financial services industry, along with the guidance of regulation and legislation such as Health Insurance Portability and Accountability Act, Section 326 of the USA PATRIOT Act and California's Senate Bill1386 (Database Protection Act of 2003), have worked to enhance its data security systems, processes and customer notification procedures. Many of the standards suggested in the Proposed Guidance have been implemented. Many of the standards are covered by other regulatory requirements applying to handling unauthorized accounts access, such as the error resolution provisions of Regulation E and Regulation Z. We believe the structure and language of the Proposed Guidance could be improved in order to reduce the likelihood that the Guidance will actually cause institutions to react to security breaches inappropriately.

The appropriate response to a security breach affecting customer information depends on the information accessed, the extent to which the accessed information can or has been used or further disclosed, and the tools available to both the financial institution and to customers to identify and address the illicit use of the customer information. The appropriate response must balance the risks of illicit use of information against the risks that the response itself may lead to greater customer cost and inconveniences. The closing of accounts, the placing of fraud alerts, and the review of files at consumer reporting agencies involve costs and inconvenience for both the customer and the financial services industry as a whole. Closed accounts must be replaced, fraud alerts may impede future transactions, and repeated access to consumer reporting agency files can become costly. Moreover, a proliferation of fraud alerts that are not related to actual fraud can dilute the effectiveness of those alerts. In time, it may become increasingly more difficult to identify real fraud, making identification of identity theft harder rather than easier.

Notification to Regulatory and Law Enforcement Agencies

The Proposed Guidance states that a financial institution should "notify its primary federal regulator when it becomes aware of an incident involving unauthorized access to or use of customer information that could result in substantial harm or inconvenience to its customers". FleetBoston recommends that the notification requirement in the Proposed Guidance be narrowed to situations where substantial harm to customers has occurred, or is likely to occur, instead of a possibility of occurring.

Furthermore, neither the role of the financial institution as a third party or service provider, nor the financial institution's use of a third party service provider is appropriately addressed. Financial institutions typically require service providers to fully disclose information relating to any breach in security resulting in an unauthorized access to, or use of, a customer's information. If the bank is acting as a service provider for another institution, its obligation is to the entity from which it received the information rather than to the subject of the information. We believe that a response program that unnecessarily mandates notification of customers and other entities, such as law enforcement and regulatory agencies, of security breaches that do not rise to the appropriate "threat level" will tend to discourage service providers from disclosing security breaches because of the potential liability and reputational risk.

Corrective Measures: Flagging Accounts

The Proposed Guidance states that financial institutions should immediately begin identifying and monitoring the accounts of customers whose information **may** have been accessed or misused. The Proposed Guidance's use of the term "may" is unclear as to what exactly would constitute a triggering event and how long such "flagging" should last. Unlike customer notification, which is required after a security breach of sensitive customer information, flagging is required after a security breach of any customer information – significantly increasing instances where special monitoring is unnecessarily required.

The financial services industry, through associations such as the American Bankers Association, Financial Forum and Consumer Bankers Association has coordinated a proactive effort to develop standards for fraud monitoring. FleetBoston believes that its existing fraud monitoring systems and risk-based procedures sufficiently protect its accounts and customers when there is a true threat to customer information security.

Corrective Measures: Secure Accounts

The Proposed Guidance states that "when a checking, savings or other deposit account number, debit or credit card account number, personal identification number, password, or other unique identifier has been accessed or misused, the financial institutions should secure the account, and all other accounts and bank services that can be accessed using the same account number or name and password combination until such time as the financial institution and the customer agree on a course of action." The meaning of "secure accounts" is unclear. If securing account means closing the account, the adverse effects on customers will be substantial. The closing or blocking of customer accounts should be done when the risks of fraud are clear and significant. The financial institution should be allowed the flexibility to determine when and how an account is "secured" by weighing the severity of the security breach. Closing a customer's account(s) in a non-threatening situation, until the customer and the financial institution can agree on a course of action, will only result in unnecessary costs and inconvenience to the customer and inefficiency to the financial institution's services and processes. We recommend the guidance include a statement regarding how the closed accounts should be reported to the credit bureaus to ensure consistency across the process and to reduce potential negative interpretations of the closure of accounts in cases of this nature.

Customer Notification and Internal Fraud Procedures

The Proposed Guidance states that a financial institution should "notify affected customers whenever it becomes aware of unauthorized access to sensitive customer information unless the institution, after appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of the affected customers, including by monitoring affected customers' accounts for unusual or suspicious activity".

FleetBoston supports the concept of customer notification in appropriate circumstances, again, following risk-based procedures. While we support the flexibility allowed the financial institution to conduct their investigation, we find the language in the Proposed Guidance to be unclear as to what constitutes a security breach. We are concerned that the Proposed Guidance could trigger the customer notification requirement unpredictably, resulting in unnecessary notification. The examples provided within the context of "appropriate triggering events" are too broad and should be narrowed in scope.

The Proposed Guidance further states that notification is required "whenever the financial institution becomes aware of unauthorized access to sensitive customer information," again increasing the risk of unnecessary notifications. Because of the short period between discovery of a security breach, and the deadline set by the Proposed Guidance for customer notification, it is likely that customer notifications will be required before an appropriate investigation can take place. We recommend that the financial institution should be allowed the discretion, after conducting reasonable investigation, to determine whether the customer should be notified.

Delivery of Notification Options

The Proposed Guidance does not adequately describe the options available to financial institutions for notification delivery. The Proposed Guidance indicates that when the financial institution can identify affected individual accounts, notice to those individuals will suffice. However, in those circumstances when the financial institution is unable to determine precisely what customers are affected, the Proposed Guidance states that financial institution should "notify each customer in groups likely to have been affected." The only delivery mechanisms mentioned are phone, mail and electronic notice. The rules for mass customer notification should provide flexibility to the financial institution to notify customers by traditional methods or through alternative methods (e.g. Internet, press release). Again, notification should be required only when investigation reveals a threat that the customer needs to address with proper safety measures.

Closing Remarks

FleetBoston appreciates the opportunity to provide you with our comments on this important issue. We support an aggressive response program to secure the information which more than 20 million customers have entrusted with us. FleetBoston is actively involved with several industry associations and forums to improve and enhance identity theft programs for our customers and financial services industry. We appreciate your efforts in beginning the development of national standards. We hope our comments will assist in this effort. If you have questions regarding our comments, please contact Coralee Harris, Privacy Group Leader, at 803-781-1082.

Sincerely,

Agnes Bundy Scanlan
Managing Director and
Chief Compliance Officer